Tasdiqlangan

«____» _____ 20__ yildagi _____son Buyruq bilan

"Unitel" MCHJ yetkazib beruvchilari va hamkorlari uchun xavfsizlik siyosati

Toshkent 2025 yil

1. Maqsadi

1.1 Ushbu siyosat kompaniyaning axborot tizimlari, ma'lumotlari va infratuzilmasidan foydalanishni talab qiladigan IT loyihalarini amalga oshirishda ishtirok etadigan yetkazib beruvchilar va hamkorlar bilan ishlashda tavsiyalar xavfsizligi standartlariga rioya etilishini ta'minlashga qaratilgan.

1.2 Siyosat axborot xavfsizligi bilan bog'liq xavflarni minimallashtirish va kompaniya va uning mijozlari ma'lumotlarini himoya qilishni ta'minlashga qaratilgan.

2. Qo'llash sohasi

"Unitel" MCHJ yetkazib beruvchilari va hamkorlari uchun kompaniyaning axborot tizimlariga kirish huquqiga ega bo'lgan IT-loyihalar, shuningdek kompaniyaning maxfiy ma'lumotlari va biznes uchun muhim ma'lumotlar qayta ishlanadigan, uzatiladigan yoki saqlanadigan loyihalar uchun xavfsizlik siyosati.

3. Asosiy talablari

3.1 Xavfsiz ishlab chiqishga talablar

3.1.1 Kompaniya uchun loyihalar ustida ishlaydigan barcha ishlab chiquvchilar xavfsiz ishlab chiqish tamoyillariga rioya qilishlari kerak, shu jumladan zaifliklarni nazorat qilish, manba kodini tahlil qilish va xavfsizlik sinovlariga – SAST\DAST\OSA.

SAST (Static Application Security Testing) — bu zaifliklar va xatolarni aniqlash uchun manba kodini statik (ishga tushirmasdan) tahlil qilish orqali ishlab chiqishning dastlabki bosqichlarida dastur kodi xavfsizligini tahlil qilish usuli.

DAST (Dynamic Application Security Testing) — bu manba kodiga kirmasdan tashqi muhitdan zaifliklarni aniqlash uchun dasturning real vaqt rejimida, ish vaqtida ishlashini tahlil qilish orqali xavfsizligini sinash usuli.

OSA (Open Source Analysis) — bu zaifliklar, litsenziyalar va xavfsizlik talablariga muvofiqligi yuzasidan loyihada ishlatiladigan ochiq komponentlar va kutubxonalarni tahlil qilish va baholash jarayoni.

3.1.2 Loyihalar SQL-inyeksiyalar, XSS va boshqa zaifliklarni o'z ichiga olgan asosiy tahdidlardan himoya qilish uchun OWASP (Open Web Application Security Project) kabi xavfsiz ishlab chiqish standartlarini hisobga olgan holda ishlab chiqilishi kerak.

OWASP (Open Web Application Security Project) — bu tavsiyalar, standartlar va vositalarni nashr etish orqali veb-ilovalar xavfsizligini yaxshilash bilan shug‘ullanadigan ochiq xalqaro tashkilot.

SQL-inyeksiya — bu buzg‘unchi shaxs ma'lumotlar bazasiga ruxsatsiz kirish yoki uni o'zgartirish uchun kiritilgan ma'lumotlarga zararli SQL-so'rovlarni kiritadigan zaiflik turi.

XSS (Cross-Site Scripting) — bu veb-ilovalarning zaifligi bo'lib, unda buzg‘unchi shaxs boshqa foydalanuvchilarning brauzerida bajarish va ma'lumotlarni o'g'irlash yoki sayt ishini buzish uchun veb-sahifaga zararli skriptni kiritadi.

3.1.3 Koddagi barcha o'zgarishlar xavfsizlik jihatlarini hisobga olgan holda kod-revyudan o‘tishi kerak.

3.2 Parollarga qo‘yiladigan talablar

Kompaniya infratuzilmasiga ulangan barcha foydalanuvchilar va tizimlar korporativ talablarga javob beradigan murakkab parollardan foydalanishlari kerak.

3.2.1 **OWASP (Open Web Application Security Project)** — bu tavsiyalar, standartlar va vositalarni nashr etish orqali veb-ilovalar xavfsizligini yaxshilash bilan shug‘ullanadigan ochiq xalqaro tashkilot.

3.2.2 Parolning minimal uzunligi harflar, raqamlar va maxsus belgilar kombinatsiyasini o'z ichiga olgan 12 belgidan iborat bo'lishi kerak.

3.2.3 Parollar har 180 kunda yangilanishi kerak va oldingi parollarni qayta ishlatish taqiqlanishi kerak.

3.2.4 Autentifikatsiya ma'lumotlari (parollar, tokenlar) ochiq ko‘rinishda yoki ilovalar kodida saqlanmasligi kerak.

Autentifikatsiya ma'lumotlari (parollar, tokenlar) — bu foydalanuvchining shaxsini tasdiqlash va tizimlar yoki ma'lumotlarga kirish uchun ishlatiladigan ma'lumotlar.

3.3 PAM orqali kompaniya infratuzilmasiga kirishni boshqarish

3.3.1 Muhim tizimlar va ma'lumotlarga kirish bilan bog'liq barcha harakatlar faqat imtiyozlarni boshqarish yechimlari (PAM) orqali amalga oshirilishi kerak.

PAM (Privileged Access Management) — bu ruxsatsiz foydalanishning oldini olish va xavfsizlikni oshirish uchun yuqori imtiyozli hisobl yozuvlariga kirishni boshqarish va nazorat qilish tizimi va jarayonlari.

3.3.2 Imtiyozli hisob yozuvlariga kirish ruxsati faqat muayyan vazifalarni bajarish uchun vaqtincha berilishi va qat'iy nazorat qilinishi kerak.

3.3.3 PAM (Privileged Access Management) orqali barcha operatsiyalar keyingi audit uchun qayd etilishi kerak.

3.4 Loglarni SIEM-ga uzatish talablari

SIEM (Security Information and Event Management) — bu hodisalarni aniqlash va ularga javob berish uchun turli manbalardan xavfsizlik ma'lumotlarini yig'ish, tahlil qilish va korrelyatsiya qilish tizimi.

3.4.1 Yetkazib beruvchilar va hamkorlar tomonidan ishlatiladigan barcha tizimlar loglarni korporativ axborot xavfsizligi hodisalarini boshqarish tizimiga (SIEM) o'tkazish uchun sozlanishi kerak.

3.4.2 Loglarning tarkibiga kirishga urinishlar, yuqori imtiyozli harakatlar, tizimdagi muhim o'zgarishlar va boshqa muhim voqealar to'g'risidagi ma'lumotlar kiritilishi kerak.

3.4.3 Loglar modifikatsiyadan himoyalangan bo'lishi va faqat saqlash qoidalariga muvofiq o‘chirilishi kerak.

3.5 Zaifliklarni aniqlash uchun EDR va agentlarni joylashtirish talablari

3.5.1 Yetkazib beruvchilar va hamkorlar so'nggi qurilmalarda (EDR) tahdidlarni aniqlash va hodisalarga javob berish yechimlarini o'rnatish va ulardan foydalanishni qo'llab-quvvatlashlari kerak.

EDR (Endpoint Detection and Response) — bu hujumlarni tezda aniqlash, tahlil qilish va yo'q qilish uchun oxirgi qurilmalarda (kompyuterlar, serverlar) tahdidlarni kuzatish va ularga javob berish texnologiyasi.

3.5.2 Korporativ ma'lumotlar va tizimlarga kirish uchun ishlatiladigan barcha ishchi stansiyalar va serverlarda zaifliklarni aniqlash agentlari bo'lishi kerak, ular muntazam ravishda yangilanadi va zaifliklar borligi yuzasidan tizimlarni skanerlaydi.

3.5.3 Yetkazib beruvchilar o'z tizimlarida aniqlangan barcha zaifliklarni darhol bartaraf etishlari shart.

3.5.4 Xavfsizlik yangilanishlarini qo'llab-quvvatlamaydigan serverlar, operatsion tizimlar va dasturlardan foydalanish taqiqlanadi.

DT (dasturiy ta'minot) — bu kompyuterlar va boshqa qurilmalarda muayyan vazifalarni bajarish uchun mo'ljallangan dasturlar va ma'lumotlar to'plami.

3.6 Ikki faktorli autentifikatsiya talablari (2FA)

3.6.1 Korporativ tizimlarga kiradigan barcha foydalanuvchilar ikki faktorli autentifikatsiyadan (2FA) foydalanishlari shart.

2FA (ikki faktorli autentifikatsiya) — bu hisob yozuvini himoya qilish usuli bo‘lib, unda tizimga kirish uchun ikki xil shaxsni tasdiqlovchi omil talab qilinadi, masalan, SMS yoki ilovadan parol va kod.

3.6.2 2FA barcha masofaviy ulanishlar va sezgir tizimlarga kirish uchun sozlanishi kerak.

3.6.3 2FA usullari sifatida OTP, biometriya, apparat tokenlari yoki boshqa xavfsiz yechimlardan foydalanish tavsiya etiladi.

OTP (One-Time Password) — faqat bitta sessiya yoki kirish uchun amal qiladigan bir martalik parol, odatda SMS orqali yuboriladi yoki ilovada yaratiladi.

Biometriya— foydalanuvchining barmoq izi, yuzi yoki ovozi kabi noyob jismoniy xususiyatlariga asoslangan autentifikatsiya usuli.

Uskuna tokenlari — qo'shimcha xavfsizlik omili sifatida ishlatiladigan kodlarni yaratadigan yoki kirishni tasdiqlovchi jismoniy qurilmalar.

3.7 Xavfsiz protokollardan foydalanish talablari

3.7.1 Autentifikatsiya, avtorizatsiya va ma'lumotlarni uzatish uchun faqat OAuth 2.0, SAML, TLS 1.2 kabi yoki undan yuqori xavfsiz protokollardan foydalanish kerak.

OAuth 2.0 — parollarni uzatmasdan resurslarga xavfsiz kirish imkonini beruvchi avtorizatsiya protokoli.

SAML — yagona kirish tizimlari (SSO) o'rtasida autentifikatsiya va avtorizatsiya ma'lumotlarini almashish standarti.

TLS 1.2— shifrlash va ulanish xavfsizligini ta'minlaydigan tarmoq orqali uzatishda ma'lumotlarni himoya qilish protokoli.

3.7.2 Barcha ma'lumotlarni uzatish shifrlangan bo'lishi, HTTP va FTP kabi eskirgan va xavfli protokollar esa o'chirib qo'yilishi kerak.

HTTP (HyperText Transfer Protocol) — internetda veb-sahifalarni yuklash va namoyish qilish uchun ma'lumotlarni uzatish protokoli.

FTP (File Transfer Protocol) — tarmoqdagi kompyuterlar o'rtasida fayllarni uzatish protokoli.

3.7.3 API-shifrni ochishga kirish va kompaniya tizimlari bilan integratsiyalash tokenlar, kirish kalitlari va so'rovlarni autentifikatsiya qilish va avtorizatsiya qilishni ta'minlaydigan boshqa usullar bilan himoyalangan bo'lishi kerak.

API (Application Programming Interface) — bu turli xil dasturlarga o'zaro aloqa qilish va o'zaro ma’lumotlar almashish imkonini beradigan qoidalar va vositalar to'plami.

3.7.4 Yechimlar Active Directory integratsiyasini xavfsiz protokollar – Kerberos, Ldaps bilan qo'llab-quvvatlashi kerak.
Active Directory (AD) — bu korporativ tarmoqdagi foydalanuvchilar, kompyuterlar va resurslarni boshqarish uchun Microsoft-ning kataloglar xizmati bo'lib, u markazlashtirilgan autentifikatsiyani va kirishni nazorat qilishni ta’minlaydi.

Kerberos — bu chiptalar tizimi orqali tarmoqdagi foydalanuvchilarning shaxsini xavfsiz tasdiqlashni ta'minlaydigan autentifikatsiya protokoli.

LDAPS (LDAP) — shifrlash yordamida katalog xizmatlarida ma'lumotlarga xavfsiz kirish va boshqarish uchun himoyalangan protokol.

3.8 Veb-servislar uchun WAF-dan foydalanish talablari

3.8.1 Yetkazib beruvchilar yoki hamkorlar tomonidan ishlab chiqiladigan va qo'llab-quvvatlanadigan barcha veb-servislar Web Application Firewall (WAF) yordamida himoyalangan bo'lishi kerak.

WAF (Web Application Firewall) — bu veb-ilovalarga hujumlarning oldini olish uchun zararli trafikni filtrlaydigan va bloklaydigan veb-servislarni himoya qilish tizimi.

3.8.2 WAF SQL-inyeksiyalar, XSS, RFI kabi va OWASP tomonidan aniqlangan boshqa tahdid turlari hujumlarini aniqlaydigan va blokirovka qiladigan tarzda sozlanishi kerak.

RFI (Remote File Inclusion) — bu veb-ilovaning zaifligi bo'lib, unda buzg‘unchi shaxs serverda o'chirilgan faylni ulashi va bajarishi mumkin, bu esa tizimning buzilishiga olib keladi.

3.8.3 WAF konfiguratsiyasi yangi zaifliklardan himoya qilish uchun vaqti-vaqti bilan yangilanishi kerak va veb-servislarda yangi funksiyalar yoki o'zgartirishlar kiritilishidan oldin sinovdan o'tkazilishi kerak.

3.9 Shaxsiy ma'lumotlarni shifrlash bo‘yicha ma'lumotlar bazalariga qo'yiladigan talablar

3.9.1 Shaxsiy ma'lumotlar yoki kompaniyaning sezgir ma'lumotlarini o'z ichiga olgan barcha ma'lumotlar bazalari ma'lumotlarni saqlash darajasidagi shifrlashdan (at-rest) foydalanishi kerak.

At-rest saqlash — bu ma'lumotlarning tinch holatda saqlanishi, ya'ni ma'lumotlar tashuvchi qurilmalarda saqlanadi va tarmoq orqali uzatilmaydi, ruxsatsiz kirishdan himoya qilishni talab qiladi.

3.9.2 Ma'lumotlarni shifrlash zamonaviy kriptografik algoritmlar yordamida amalga oshirilishi kerak (masalan AES-256), tarqalib ketish holatlarida ma'lumotlarni himoya qilish uchun protokol turi.

AES-256 — uzunligi 256 bit kalit bilan ma'lumotlarni simmetrik shifrlash standarti bo'lib, axborotni yuqori darajadagi himoya bilan ta’minlaydi.

3.9.3 Shifrlash kalitlariga kirish cheklangan bo‘lishi va kalitlarni boshqarish tizimi (KMS, Key Management System) orqali boshqarilishi kerak.

KMS (Key Management System) — kriptografik kalitlarni boshqarish tizimi bo‘lib, ma'lumotlarni himoya qilish uchun ularni yaratish, saqlash, taqsimlash va kirish nazoratini ta'minlaydi.

3.9.4 Shaxsiy ma'lumotlar uzatilganda (in-transit) ular ham xavfsiz protokollar (masalan, TLS 1.2 va undan yuqori) yordamida shifrlanishi kerak.

(In-transit) - bu qurilmalar o'rtasida tarmoq orqali uzatiladigan va uzatish paytida ushlab qolish va o'zgarishlardan himoya qilishni talab qiladigan ma'lumotlar.

3.9.5 Yetkazib beruvchilar shifrlash talablarini bajarish uchun muntazam tekshiruvlar o'tkazishlari va kerak bo'lganda hisobotlarni taqdim etishlari shart.

4. Javobgarlik

Xarid qilish tadbirlari uchun texnik topshiriqni tuzishda **loyiha Menejerlari/buyurtmachilar** kompaniyaning Axborot xavfsizligi bo'limi bilan talablarni qo‘llaniladigan loyihalarda kelishib olishlari kerak. Xarid qilish, Shartnomalar va Logistika Xizmatiga ariza berishda barcha zarur talablar hujjatlarda aks ettirilishi kerak.

Yetkazib beruvchilar va hamkorlar ushbu siyosat talablariga rioya qilishlari va ularning xodimlari va pudratchilari barcha xavfsizlik talablarini bajarishlarini ta'minlashlari shart. Shu o‘rinda, xarid qilish tadbirini boshlash paytida zarur talablarni kiritish to'g'risidagi yuqoridagi band bajarilishi kerak.

Kompaniyaning axborot xavfsizligi bo'limi siyosatning bajarilishini nazorat qilish, auditlar o'tkazish va belgilangan standartlarga rioya qilishini tekshirish uchun javob beradi.

5. Istisnolar

5.1 Agar kompaniyaning etkazib beruvchilari va hamkorlari ushbu siyosatda nazarda tutilgan usullardan farq qiladigan axborot tizimlarini himoya qilishning muqobil usullarini taklif qilsalar, bunday usullar bir vaqtning o'zida quyidagi shartlarga rioya qilgan holda qo'llanilishi mumkin:

- axborot tizimlarini himoya qilishning ko‘rsatilgan muqobil usullari ushbu siyosatda nazarda tutilgan himoya darajasiga teng yoki undan yuqori himoya darajasini ta'minlaydi;
- bunday muqobil usullardan foydalanish Kompaniyaning axborot xavfsizligi bo'limi bilan oldindan kelishilgan.

6. Nazorat va audit

6.1 Kompaniya ichki axborot xavfsizligi protseduralariga muvofiq ushbu talablarning bajarilishini tekshirish, shu jumladan tizimlarning zaifliklarini har oyda skanerlash va kirishlarni nazorat qilish uchun vaqti-vaqti bilan xavfsizlik auditlarini o'tkazish huquqini o'zida saqlab qoladi.

7. Qoidabuzarliklar va javobgarlik

7.1 Yetkazib beruvchilar va hamkorlar O'zbekiston Respublikasining amaldagi qonunchiligiga muvofiq xavfsizlik talablariga rioya qilmaslik natijasida kompaniyaga yetkazilgan zarar uchun javobgar bo'lishlari shart.